目次

はじめに

このたびは弊社の FMV パソコン（以降、パソコン本体）をご購入いただき、まことにありがとうございます。
本書は、パソコン本体に搭載されているセキュリティチップ（以降、本製品）の基本的な取り扱い、セキュリティチップを利用するためのソフトウェアのインストール、および設定と使い方について説明しています。
ご使用になる前に本書およびパソコン本体のマニュアルをよくお読みになり、正しい取り扱いをされますようお願いいたします。

2006 年 1 月

■セキュリティ機能について

セキュリティ機能は完全な認証照合、データやハードウェアの保護を保証するものではありません。当社は、お客様がセキュリティ機能を使用されたこと、または使用できなかったことによって生じるいかなる損害に関しても、一切の責任を負いかねますのであらかじめご了承ください。

本書の表記

本文中に記載されている記号には、次のような意味があります。

記号	意味
重要	お使いになる際の注意点や、してはいけないことを記述しています。必ずお読みください。
POINT	操作に関連することを記述しています。必要に応じてお読みください。
→	参照ページや参照マニュアルを示しています。

■コマンド入力（キー入力）

CD/DVD ドライブなどのドライブ名を、［CD/DVD ドライブ］で表記しています。入力の際は、お使いの環境に合わせて、ドライブ名を入力してください。
例：[CD/DVD ドライブ]：¥setup.exe

■連続する操作の表記

本文中の操作手順において、連続する操作手順を、「→」でつなげて記述しています。

例：　「スタート」ボタンをクリックし、「すべてのプログラム」をポイントし、「アクセサリ」をクリックする操作

↓

「スタート」ボタン→「すべてのプログラム」→「アクセサリ」の順にクリックします。

■製品の呼び方

本文中の製品名称を、次のように略して表記します。
なお、本書ではお使いの機種、または OS 以外の情報もありますが、ご了承ください。

<table>
<tr><th>製品名称</th><th colspan="4">本文中の表記</th></tr>
<tr><td>FMV-W5210</td><td>W5210</td><td rowspan="7">FMV-ESPRIMO</td><td rowspan="22" colspan="2">パソコン本体</td></tr>
<tr><td>FMV-E5210</td><td>E5210</td></tr>
<tr><td>FMV-D5310</td><td>D5310</td></tr>
<tr><td>FMV-D5210</td><td>D5210</td></tr>
<tr><td>FMV-D5110</td><td>D5110</td></tr>
<tr><td>FMV-B5210</td><td>B5210</td></tr>
<tr><td>FMV-K5210</td><td>K5210</td></tr>
<tr><td>FMV-H8210</td><td>H8210</td><td rowspan="11">FMV-LIFEBOOK</td></tr>
<tr><td>FMV-E8310</td><td>E8310</td></tr>
<tr><td>FMV-E8210</td><td>E8210</td></tr>
<tr><td>FMV-E8110</td><td>E8110</td></tr>
<tr><td>FMV-C8210</td><td>C8210</td></tr>
<tr><td>FMV-S8215</td><td>S8215</td></tr>
<tr><td>FMV-S8210</td><td>S8210</td></tr>
<tr><td>FMV-B8210</td><td>B8210</td></tr>
<tr><td>FMV-T8210</td><td>T8210</td></tr>
<tr><td>FMV-P8210</td><td>P8210</td></tr>
<tr><td>FMV-C6310</td><td>C6310
バリューライン</td></tr>
<tr><td>FMV-STYLISTIC TB12/S</td><td>TB12/S</td><td rowspan="3">FMV-STYLISTIC</td></tr>
<tr><td>FMV-STYLISTIC TB12/B</td><td>TB12/B</td></tr>
<tr><td>FMV-STYLISTIC TB12/R</td><td>TB12/R</td></tr>
<tr><td>FMV-N5210FA</td><td>N5210FA</td><td>FMV FA パソコン</td></tr>
<tr><td>Microsoft® Windows® XP Professional</td><td colspan="2">Windows XP Professional</td><td rowspan="3">Windows XP</td><td rowspan="3">Windows</td></tr>
<tr><td>Microsoft® Windows® XP Home Edition</td><td colspan="2">Windows XP Home Edition</td></tr>
<tr><td>Microsoft® Windows® Tablet PC Edition 2005</td><td colspan="2">Windows XP Tablet PC Edition 2005</td></tr>
<tr><td>SMARTACCESS/Basic</td><td colspan="4" rowspan="2">SMARTACCESS</td></tr>
<tr><td>SMARTACCESS/Premium</td></tr>
<tr><td>Microsoft® Internet Explorer</td><td colspan="4">Internet Explorer</td></tr>
<tr><td>Microsoft® Word</td><td colspan="4">Word</td></tr>
<tr><td>Microsoft® Outlook®</td><td colspan="4">Outlook</td></tr>
<tr><td>Microsoft® Outlook® Express</td><td colspan="4">Outlook Express</td></tr>
<tr><td>Netscape® または Netscape® Communicator</td><td colspan="4">Netscape</td></tr>
</table>

商標および著作権について

Microsoft、Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Netscapeは、米国およびその他の国におけるNetscape Communications Corporation社の登録商標です。
FeliCa は、ソニー株式会社の登録商標です。
FeliCa は、ソニー株式会社が開発した非接触 IC カードの技術方式です。
その他の各製品名は、各社の商標、または登録商標です。
その他の各製品は、各社の著作物です。

画面の使用に際して米国 Microsoft Corporation の許諾を得ています。

使用上のご注意

■セキュリティチップで利用する鍵や証明書、パスワードの管理について

セキュリティチップは、複数の鍵や証明書を扱います。これらの鍵や証明書を紛失した場合は、その鍵によって暗号化されたファイルなどは利用できなくなることがありますので注意してください。またこれらの鍵を利用する場合はパスワードが必要です。パスワードを正しく入力しないと鍵が利用できないため、紛失時と同様に暗号化されたファイルなどが利用できなくなります。

■セキュリティチップ利用についてのご注意

・本製品で使用するソフトウェアをインストールするときには、パソコン本体またはネットワーク上のパソコンに、CD-ROM ドライブが搭載または接続されている必要があります。

・セキュリティチップで鍵を生成する場合、数分かかることがあります。

・SMARTACCESSのご利用については、SMARTACCESSのマニュアルを参照してください。

POINT

▶ SMARTACCESS のマニュアルは、それぞれ次のものをご覧ください。

- 「SMARTACCESS/Basic」をお使いの場合
  添付の「ドライバーズディスク」内の「¥other¥smartaccess¥sabasic¥manual」にあるマニュアル
- 「SMARTACCESS/Premium」をお使いの場合
  添付の「SMARTACCESS/Premium」CD-ROM 内の「¥sapremium¥manual」にあるマニュアル

・パソコン本体の修理・保守を依頼する場合は、SMARTACCESS による Windows ログオンを解除してください。
SMARTACCESS による Windows ログオンを解除していない場合、修理・保守ができないことがあります。SMARTACCESS による Windows ログオンを解除するには、次の手順を行ってください。

1. SMARTACCESS をインストールしたユーザで Windows にログオンします。
2. 「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。
   「環境設定」が表示されます。
3. 「ログオン認証」－「Windows ログオン」の順にクリックします。
4. 「SMARTACCESS による Windows ログオン」の「使用しない」にチェックし、「OK」をクリックします。

・パソコン本体の修理・保守が行われた場合には、セキュリティ機能が解除されていることがあります。その場合には環境の再構築が必要となります。正しく再構築がされない場合、暗号化されたファイルやメールが復元できなくなる場合があります。

1 概要

■ セキュリティチップとは

セキュリティチップは、TCG[注1] の仕様に基づいた TPM[注2] と呼ばれる IC チップで TCG セキュリティの基本機能を提供します。セキュリティチップを搭載したパソコンは、ソフトウェアによる攻撃および物理的な攻撃からデータを保護し、より強固なセキュリティを実現します。

注 1：TCG は Trusted Computing Group の略称です。
TCG は、信頼性と安全性を持った新しいコンピュータをつくるためのオープンな業界仕様を策定する団体です。
（https://www.trustedcomputinggroup.org/）

注 2：TPM は Trusted Platform Module の略称です。

■ セキュリティチップの機能

セキュリティチップは、各ユーザに固有の鍵を生成し、証明書を管理します。この鍵と証明書を用いることにより、セキュリティチップは暗号化や認証を行います。セキュリティチップ内に保有する鍵は、取り出すことが不可能なため鍵の解読ができません。そのため暗号化されたデータや認証は安全に行われます。ユーザはこの鍵と証明書を利用するためのパスワードを設定します。

■ セキュリティチップの利用

セキュリティチップを利用するために、次のソフトウェアおよび証明書を使用します。

・Infineon TPM Professional Package（Infineon Security Platform）ユーティリティ
・SMARTACCESS
・VeriSign 証明書

これらのソフトウェアおよび証明書により、次のことが行えるようになります。

□ IEEE802.1x 認証ファイルの管理

IEEE802.1x にて利用する証明書をセキュリティチップで管理することができます。

□ ファイルとフォルダの暗号化 -EFS（Encrypting File System）

ユーティリティでファイルとフォルダの暗号化を設定することにより、EFS による暗号化に利用される鍵をセキュリティチップで安全に保管します。

重要

- EFS を利用するには、ハードディスクが NTFS でフォーマットされている必要があります。
- Windows XP Home Edition では、EFS は利用できません。
- ハードディスク全体またはボリューム全体を、暗号化することはできません。
- 特定のフォルダを暗号化すると Windows が起動しなくなる場合があります。詳しくは、添付の「セキュリティチップをご利用のお客様へ」をご覧ください。

□ セキュア E-Mail

ユーティリティで E-Mail の保護を設定することにより、E-Mail の暗号用の証明書をセキュリティチップで安全に管理します。

□ Word マクロへの署名

ユーティリティでセキュリティ機能を設定することにより、Word マクロへの署名をセキュリティチップで安全に保護します。

□ Windows ログオンにセキュリティチップを利用する

SMARTACCESS による Windows ログオンを設定することにより、Windows ログオン時のパスワードをセキュリティチップで安全に保存することができます。

重要

- 他のアプリケーションでWindowsログオンを行っている場合には、同時にSMARTACCESSによる Windows ログオンを行うことができません。一度、他のアプリケーションでの Windows ログオンを解除する必要があります。

□ パソコンの不正なハードウェアの変更の検出

SMARTACCESS の「機器監査」機能を利用すれば、Windows ログオン時パソコンの機器構成のチェックを行います。ハードウェア構成または設定が不正に変更されていることを検出した場合は、Windows ログオンを許可しないようにすることができます。

□ ID・パスワード入力をセキュリティチップで管理する

次の場合に、ID・パスワードを SMARTACCESS に登録しておくと、セキュリティチップによって保護されるため安全に管理することができます。

・アプリケーションによりポップアップ画面に表示される ID・パスワード入力要求

・Internet Explorer によりホームページに表示される ID・パスワード入力要求

また、一度登録すると、ID・パスワードのフォームは自動で認識され、再び手入力することなく利用できます。

□ シングルサインオンを利用する

SMARTACCESS にはシングルサインオンの機能があります。一度セキュリティチップのパスワードを入力するか、SMARTACCESS による Windows ログオンを行えば、SMARTACCESS が管理する ID やパスワードは自動で入力されます。

□ VeriSign 証明書の利用

セキュリティチップと連携した VeriSign 発行の証明書を、登録した日から 1 年間無料で利用できます。これを利用することにより、例えばセキュア E-mail を利用する場合などは、VeriSign 認証局に証明された証明書を利用できるため、より安全なデータを送受信することができます。

POINT

- VeriSign 証明書は、セキュリティチップのユーティリティをインストールし、設定を完了して利用可能にしてからインストールを行ってください。インストールについては、それぞれ次のファイルをご覧ください。
  - 「SMARTACCESS/Basic」をお使いの場合
    添付の「ドライバーズディスク」内にある「¥other¥smartaccess¥ifxsw20¥versign.txt」
  - 「SMARTACCESS/Premium」をお使いの場合
    添付の「SMARTACCESS/Premium」CD-ROM 内にある「¥ifxsw20¥versign.txt」
- VeriSign 証明書は、登録した日から 1 年間利用できます。それ以降は、E-mail などで証明書を利用することはできません。ただし、古いメールなどで利用していた場合には、読むことのみ可能です。
- 1 年間の利用期間終了後もご利用を希望の場合は、弊社担当営業員までご連絡ください。その場合有料による継続となります。

□ 他のセキュリティ機能と連携した利用

セキュリティチップは、他のセキュリティ機能と連携した利用が可能です。連携できるセキュリティ機能には、次のものがあります。

・指紋センサー

・FeliCa 対応リーダ／ライタ

POINT

- 指紋センサーとの連携には「SMARTACCESS/Basic」または「SMARTACCESS/Premium」が必要です。
- 指紋認証装置との連携はできません。
- FeliCa 対応リーダ / ライタとの連携には「SMARTACCESS/Premium」が必要です。
- 「SMARTACCESS/Premium」には「SMARTACCESS/Basic」の機能が含まれるため、同時に使用することができません。
  「SMARTACCESS/Premium」を利用する場合は「SMARTACCESS/Basic」をインストールしないでください。
  なお、「SMARTACCESS/Basic」がすでにインストールされている場合は一度「SMARTACCESS/Basic」をアンインストールしてから「SMARTACCESS/Premium」をインストールしてください。
- 他のセキュリティ機能との連携の方法などは、次のSMARTACCESSのマニュアルをご覧ください。
  ・「SMARTACCESS/Basic」をお使いの場合
  添付の「ドライバーズディスク」内の「¥other¥smartaccess¥sabasic¥manual」にあるマニュアル
  ・「SMARTACCESS/Premium」をお使いの場合
  添付の「SMARTACCESS/Premium」CD-ROM 内の「¥sapremium¥manual」にあるマニュアル

■ セキュリティチップの管理

セキュリティチップには、セキュリティチップの管理を行う「所有者」とセキュリティチップを使用する「ユーザ」を登録します。
所有者およびユーザは次の鍵および証明書やファイルを作成・利用します。

□「所有者」が管理するもの

所有者キーと所有者パスワード

所有者は、所有者であることを証明するキーを作成します。この鍵はセキュリティチップにより保護され、所有者パスワードを入力することによって利用することができます。
所有者パスワードは忘れないよう注意してください。

自動バックアップファイルと復元用トークン

セキュリティチップで管理しているすべての鍵や証明書のバックアップを行います。
バックアップはスケジュールを設定することにより定期的に行うことができます。
セキュリティチップが故障しても、新しいパソコンでこのファイルを用いて復元することにより、以前利用していた暗号化ファイルなどが利用できるようになります。
自動バックアップファイルは、トークンにより暗号化されています。自動バックアップファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

パスワードリセットファイルとリセットトークン

ユーザがセキュリティチップのパスワードを忘れた場合に備え、現状のパスワードを新規パスワードに変更することができます。パスワードの変更はユーザが行います。所有者はパスワードリセットファイルを発行することにより、ユーザにパスワード変更の許可を与えます。

パスワードリセットファイルは、トークンにより暗号化されています。パスワードリセットファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

□「ユーザ」が管理するもの

ユーザーキーとユーザーキーパスワード

ユーザはセキュリティチップを利用する場合、ユーザーキーを作成します。このキーはセキュリティチップにより保護され、ユーザーキーパスワードを入力することによって利用することができます。キーを紛失した場合は、それ以前に暗号化していたデータやファイルなどを再び利用することができなくなります。管理には注意してください。また、パスワードを忘れた場合も、キーが利用できなくなるため、それまでに暗号化していたデータやファイルを再び利用することができなくなります。パスワードは忘れないよう注意してください。

パスワードリセットファイル

ユーザがセキュリティチップのパスワードを忘れた場合に備えて、現状のパスワードを新規パスワードに変更することができます。このため前もってパスワードリセット用のファイルを作成しておきます。

キーのバックアップ

キーを紛失した場合に備えて、バックアップファイルを作成することが可能です。バックアップファイルはユーザーキーパスワードによって保護されます。

2 動作条件

本製品をご使用になる前に、次の条件を確認してください。

■ 対応機種／ OS

本製品が搭載されている機種／ Windows XP

POINT

- WEB ページをご覧になるためのアプリケーションとして、Internet Explorer 6.0 以降または Netscape 4.78/7.0 以降が必要です。
- セキュア E-mail を利用するには、Outlook 2000/2002 以降、Outlook Express 6.0 以降、または Netscape 4.78/7.0 以降が必要です。
- Word マクロへの署名を利用するには、Word 2000/2002 以降が必要です。
- VeriSign 証明書を利用するには、Internet Explorer 6.0 または Netscape 4.78/7.0 が必要です。
- SMARTACCESS での、アプリケーションによりポップアップ画面に表示される ID・パスワード入力要求機能は、Netscape ではお使いになれません。

3 作業の流れ

本製品を使用するまでの手順は次のとおりです。

1 必要なものを用意します。

・パソコン本体
・ドライバーズディスク

2 BIOS の設定を変更します。

「BIOS の設定を変更する」（→ P.12）

1. BIOS の「管理者用パスワード」を設定します（W5210 以外の場合）。
2. 「Security Chip」または「セキュリティチップ」の項目を「Enabled」または「使用する」に設定します。

3 ソフトウェアのインストールと設定を行います。

「ソフトウェアのインストールと設定を行う」（→ P.15）

重要

- セキュリティチップ、または指紋センサーのどちらかのみを設定してインストール後、両方の機能を使用したい場合は SMARTACCESS を一度アンインストールし、それぞれの設定を行ってから再度 SMARTACCESS をインストールする必要があります。
- 「SMARTACCESS/Premium」には「SMARTACCESS/Basic」の機能が含まれるため、同時に使用することができません。
「SMARTACCESS/Premium」を利用する場合には「SMARTACCESS/Basic」をインストールしないでください。
なお、「SMARTACCESS/Basic」がすでにインストールされている場合は、一度アンインストールしてから「SMARTACCESS/Premium」をインストールしてください。

POINT

- セキュリティチップを使用する場合、SMARTACCESS をインストールする前に BIOS の設定と Infineon TPM Professional Package（Infineon Security Platform）ユーティリティのインストールが必要です。また指紋センサーを使用する場合、SMARTACCESS をインストールする前に指紋センサーのドライバのインストールが必要です。
インストールの方法については、SMARTACCESS のマニュアルをよくお読みになり、手順に従って行ってください。

4 インストールと設定について

BIOS の設定を変更する

本製品を使用する前に、必ず BIOS の設定を変更してください。

・「W5210 の場合」(→ P.12)
・「E5210、D5310、D5210、D5110、B5210、K5210、N5210FA の場合」(→ P.13)
・「FMV-LIFEBOOK、FMV-STYLISTIC の場合」(→ P.14)

POINT

- BIOS セットアップについては、パソコン本体の『FMV マニュアル』の「BIOS」を参照してください。

■ W5210 の場合

1 **パソコン本体の電源を入れ、BIOS セットアップを起動します。**
BIOS セットアップ画面が表示されます。

2 **Secrity メニューで「Embedded Security Chip」を選択して、【Enter】キーを押します。**
設定変更画面が表示されます。

3 **【↑】キーまたは【↓】キーを押して、「Enabled」に設定します。**

4 **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**

5 **【↑】キーまたは【↓】キーを押して「Save Changes & Exit」を選択し、【Enter】キーを押します。**
「Save Configuration Changes and exit now?」ウィンドウが表示されます。

6 **【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。**
BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- セキュリティチップの設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。

■ E5210、D5310、D5210、D5110、B5210、K5210、N5210FA の場合

1 パソコン本体の電源を入れ、BIOS セットアップを起動します。

BIOS セットアップ画面が表示されます。
BIOS セットアップで管理者用パスワードを設定している場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。

重要

- 本製品を使用するには、BIOS セットアップで管理者用パスワードを設定する必要があります。

2 Security メニューで「Set Supervisor Password」を選択して、【Enter】キーを押します。

パスワード入力用のウィンドウが表示されます。

3 8 桁までのパスワードを入力します。

入力できる文字種はアルファベットと数字です。
入力された文字は表示されず、代わりに「■」が表示されます。

4 パスワードを入力したら、【Enter】キーを押します。

「Confirm New Password」にカーソルが移り、パスワードの再入力を求められます。

5 手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。

「Setup Notice」と書かれたウィンドウが表示されます。

6 【Enter】キーを押します。

再入力したパスワードが間違っていた場合は、「Setup Warning」ウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。

7 【↑】キーまたは【↓】キーでカーソルを移動し、「Security Chip Setting」を選択して【Enter】キーを押します。

設定変更画面が表示されます。

8 【Space】キーまたは【−】キーを押して、「Security Chip」の項目を「Enabled」に設定します。

9 Exit メニューが表示されるまで、何度か【Esc】キーを押します。

10 【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。

「Save Configuration Changes and exit now?」ウィンドウが表示されます。

11 【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- セキュリティチップの設定を有効にするには、BIOSセットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「Exit Saving Changes」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

■ FMV-LIFEBOOK、FMV-STYLISTIC の場合

1 パソコン本体の電源を入れ、BIOS セットアップを起動します。

BIOS セットアップ画面が表示されます。

BIOS セットアップで管理者用パスワードを設定している場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。

重要

- 本製品を使用するには、BIOSセットアップで管理者用パスワードを設定する必要があります。

2 セキュリティメニューで「管理者用パスワード設定」を選択して、【Enter】キーを押します。

パスワード入力用のウィンドウが表示されます。

3 8 桁までのパスワードを入力します。

入力できる文字種はアルファベットと数字です。

入力された文字は表示されず、代わりに「■」が表示されます。

4 パスワードを入力したら、【Enter】キーを押します。

「新しいパスワードを確認してください。」にカーソルが移り、パスワードの再入力を求められます。

5 手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。

「セットアップ通知」と書かれたウィンドウが表示されます。

6 【Enter】キーを押します。

再入力したパスワードが間違っていた場合は、「セットアップ警告」ウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。

7 【↑】キーまたは【↓】キーでカーソルを移動し、「セキュリティチップ設定」を選択して【Enter】キーを押します。

「セキュリティチップ設定」が表示されます。

POINT

- E8310 では、「セキュリティチップ設定」－「セキュリティチップの状態」に、現在のセキュリティチップの動作状況が表示されます。セキュリティチップが使用可能な場合は、「有効、使用可」と表示されます。

8 【Space】キーまたは【－】キーを押して、「セキュリティチップ」の項目を「使用する」に設定します。

9 終了メニューが表示されるまで、何度か【Esc】キーを押します。

10 【↑】キーまたは【↓】キーを押して「変更を保存して終了する」を選択し、【Enter】キーを押します。

「セットアップ確認」ウィンドウが表示されます。

11 【←】キーまたは【→】キーを押して「はい」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- 「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「変更を保存する」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

ソフトウェアのインストールと設定を行う

BIOS の設定変更後、パソコン本体が再起動したら、ソフトウェアをインストールします。

重要

- ソフトウェアのインストールや設定を行うには、次のマニュアルをよくお読みになり、手順に従って行ってください。
  - ・「SMARTACCESS/Basic」をお使いの場合
    添付の「ドライバーズディスク」内の「¥other¥smartaccess¥sabasic¥manual」にあるマニュアル
  - ・「SMARTACCESS/Premium」をお使いの場合
    添付の「SMARTACCESS/Premium」CD-ROM 内の「¥sapremium¥manual」にあるマニュアル
- 「SMARTACCESS/Premium」には「SMARTACCESS/Basic」の機能が含まれるため、同時に使用することができません。
  「SMARTACCESS/Premium」を利用する場合は「SMARTACCESS/Basic」をインストールしないでください。
  なお、「SMARTACCESS/Basic」がすでにインストールされている場合は一度「SMARTACCESS/Basic」をアンインストールしてから「SMARTACCESS/Premium」をインストールしてください。
- ソフトウェアをインストールするには、管理者権限でWindowsにログオンする必要があります。
- セキュリティチップの設定（BIOS の設定とユーティリティのインストール）、または指紋センサーの設定（ドライバのインストール）のどちらかのみを行って SMARTACCESS をインストールした場合、後からもう片方の機能を使用するには、一度 SMARTACCESS をアンインストールし、セキュリティチップと指紋センサーの両方の設定を行った後、再度 SMARTACCESS をインストールする必要があります。

セキュリティチップ取扱説明書

POINT

- ソフトウェアをインストールする前に、他の使用中のアプリケーションはすべて終了させてください。
- セキュリティチップを使用する場合､SMARTACCESS をインストールする前に BIOS の設定と Infineon TPM Professional Package（Infineon Security Platform）ユーティリティのインストールが必要です。また、指紋センサーを使用する場合、SMARTACCESS をインストールする前に指紋センサーのドライバのインストールが必要です。
  インストールの方法については、SMARTACCESS のマニュアルをよくお読みになり、手順に従って行ってください。

5 運用上の注意

セキュリティチップの運用上の注意

セキュリティチップを利用するための環境設定が完了すると、ファイルやフォルダの暗号化、メールの証明書の管理などがより安全な環境で運用することができるようになります。ただし故障や修理などでパソコン本体の設定が変更された場合、セキュリティチップにより保護された情報が利用できなくなることがあります。
これらの場合に備えて、次の点に注意して運用してください。

POINT

- 次のような場合に、セキュリティチップが利用できなくなると考えられます。
  - ・セキュリティチップの故障
  - ・ハードディスクのリカバリ
  - ・パソコンの部品の交換

□ 定期的にセキュリティチップの鍵のバックアップを行う

必ずセキュリティチップによって管理されている鍵の定期的なバックアップの設定を行ってください。
バックアップファイルを紛失したり、パスワードを忘れたりすると、セキュリティチップが利用できなくなります。バックアップファイルやその時に設定したパスワードは、紛失したり忘れたりしないよう注意して管理してください。
バックアップの方法については、「バックアップについて」（→ P.18）を参照してください。

重要

- バックアップを行うと、次のファイルとパスワードが生成されます。

利用者	ファイル	ファイル名
所有者	所有者パスワード	
	システム復旧ファイル	spsystembackup.xml
	緊急時復元用トークン	spemrectoken.xml
	緊急時復元用トークンパスワード	
	パスワードリセットファイル	sppwdresetsecret.xml
	パスワードリセットトークン	sppwdresettoken.xml
	パスワードトークンパスワード	
	（基本）ユーザーパスワード	
ユーザ	（基本）ユーザーパスワード	
	パスワードリセットトークン	sppwdresetsecret.xml
	パスワードトークンパスワード	

- 復元作業は、パスワードの入力などが必要なため、弊社で行うことはできません。「リストアについて」（→ P.18）をお読みになり、注意して復元してください。

□ 機器監査を行っている場合は、修理またはハードウェア変更を行う前に SMARTACCESS による Windows ログオンを一時的に解除する

SMARTACCESSによるWindowsログオンを使用する設定にして機器監査を行っている場合、修理したり、ハードウェアの設定を変更したりすると、Windows にログオンできなくなることがあります。
必ず SMARTACCESS による Windows ログオンを使用しない設定に変更してください。変更方法については、「パソコンの修理について」（→ P.21）を参照してください。

バックアップについて

セキュリティチップで保護された環境に何らかの変更があった場合でも、引き続き以前の環境を利用するためには鍵のバックアップを行っておく必要があります。
所有者でログオンした時に、通知領域から表示される内容により、手順に従って処理を行ってください。
所有者はセキュリティチップのバックアップと各ユーザのバックアップを行う必要があります。
各ユーザでバックアップを行う必要はありませんが、復元を行った後、ユーザーキーパスワードを入力する必要があります。

重要

- バックアップの方法については、次のマニュアルにある「バックアップ」の項目をよくお読みになり、手順に従って設定してください。
  - 「SMARTACCESS/Basic」をお使いの場合
    添付の「ドライバーズディスク」内にある「SMARTACCESS/Basic リファレンスマニュアル」
  - 「SMARTACCESS/Premium」をお使いの場合
    添付の「SMARTACCESS/Premium」CD-ROM 内にある「SMARTACCESS/Premium リファレンスマニュアル」
- バックアップは、セキュリティチップの中の鍵を取り出して保存することではありません。
- バックアップ処理は、セキュリティチップを設定した時のパスワードによって保護されています。そのため、セキュリティチップを設定した人が行う必要があります。
- 手順に従ってファイルや設定変更を行わない場合、セキュリティチップで管理していた環境が利用できなくなることがあります。
- 手順は、セキュリティチップの鍵についてバックアップを行う場合の手順です。暗号化ファイルや証明書、および SMARTACCESS の設定については行われません。必要に応じて別途バックアップを行ってください。
  SMARTACCESS のバックアップについては、「SMARTACCESS/Basic リファレンスマニュアル」または「SMARTACCESS/Premium リファレンスマニュアル」の「バックアップ」の項目を参照してください。

リストアについて

リストアは、セキュリティチップで保護された環境に変更があった場合、以前の環境を引き続き利用するための作業です。
所有者はセキュリティチップのリストアを行います。
ユーザは、リストアを行う必要はありませんが、所有者がリストアを行った後にユーザーキーパスワードを入力する必要があります。

重要

- リストアの方法については、次のマニュアルにある「バックアップ」の項目をよくお読みになり、手順に従って設定してください。
  - 「SMARTACCESS/Basic」をお使いの場合
    添付の「ドライバーズディスク」内にある「SMARTACCESS/Basic リファレンスマニュアル」
  - 「SMARTACCESS/Premium」をお使いの場合
    添付の「SMARTACCESS/Premium」CD-ROM 内にある「SMARTACCESS/Premium リファレンスマニュアル」
- リストアは、セキュリティチップを設定した時のパスワードによって保護されています。そのため、リストアはセキュリティチップを設定した人が行う必要があります。
- 手順に従ってファイルや設定変更を行わない場合、セキュリティチップで管理していた環境が利用できなくなることがあります。

機器監査について

SMARTACCESS で「SMARTACCESS による Windows ログオン」を設定しておくと、パソコンの電源を入れたときやパソコンを再起動したときにハードウェアの変更を検出すると、Windows のログオンを禁止することができます。これにより、ユーザが気づかないうちに（帰宅時など）ハードウェアを変更されても、検出することができます。
なお、不正にパソコンの設定が変更されたときだけでなく、修理により設定が変更された場合でも機器監査変更が検出されることがあります。修理に出す前に「パソコンの修理について」（→ P.21）を参照し、前もって設定を変更できるようにしてください。
ハードウェアの変更については次の項目が検出されます。

重要

- 機器監査の設定方法については、次のマニュアルにある「機器監査」の項目をよくお読みになり、手順に従って設定してください。
  - 「SMARTACCESS/Basic」をお使いの場合
    添付の「ドライバーズディスク」内にある「SMARTACCESS/Basic リファレンスマニュアル」
  - 「SMARTACCESS/Premium」をお使いの場合
    添付の「SMARTACCESS/Premium」CD-ROM 内にある「SMARTACCESS/Premium リファレンスマニュアル」
- 次の変更を行う前に SMARTACCESS の「機器監査」をオフにし、変更後、再度「現在の機器構成情報の登録」を行う必要があります。
- W5210 の場合、ハードウェアや BIOS 設定の変更を元に戻しても、機器監査の状態が元に戻らないことがあります。そのため、誤って変更してしまったり、変更後に機器監査の再登録を行わなかったりすると、Windows にログオンできなくなります。その場合は、機器構成を登録し直す必要があります。

POINT

- ハードウェアの変更については、休止状態からの復帰時にも確認されます。

□ BIOS 設定変更

BIOS でハードウェア構成が変更された場合に、機器監査で通知されます。

□ メモリ構成の変更

メモリスロットの構成に変更があった場合に、機器監査で通知されます。

□ ハードディスクドライブ構成の変更（W5210 の場合）

ハードディスクドライブの構成に変更があった場合に、機器監査で通知されます。

□ PCI スロット、グラフィックボードの変更（FMV-ESPRIMO、FMV FA パソコンの場合）

PCI スロットの構成およびグラフィックボードを変更した場合に、機器監査で通知されます。

□ モバイルマルチベイ／マルチベイの変更（FMV-LIFEBOOK の場合）

モバイルマルチベイまたはマルチベイを変更した場合に、機器監査で通知されます。

□ USB デバイスの変更

USB ポートに USB メモリなどのストレージデバイスを接続した場合に、機器監査で通知されます。

POINT

- USB デバイスの変更を検出するには、BIOS セットアップで次のように設定する必要があります。
  - ・W5210 の場合
    「USB BIOS Supported Devices」: Auto または All
    ご購入時の設定は「Auto」になっています。
  - ・FMV-ESPRIMO（W5210 以外）、FMV FA パソコンの場合
    「USB Legacy Support」: Enabled
    ご購入時の設定は「Disabled」になっています。
  - ・FMV-LIFEBOOK、FMV-STYLISTIC の場合
    「レガシー USB サポート」: 使用する
    ご購入時の設定は「使用する」になっています。

  BIOS セットアップについては、パソコン本体の『FMV マニュアル』の「BIOS」を参照してください。

パソコンの修理について

パソコンを修理に出す場合、修理後の設定が修理前とは異なることがあります。そのため、修理に出す前や出した後には次の作業が必要になります。

■修理前に必要な作業

□ 鍵のバックアップ

「バックアップについて」(→ P.18)をお読みになり、バックアップを行います。

□ SMARTACCESS による Windows ログオンを使用しない設定に変更する

必ず SMARTACCESS による Windows ログオンを使用しない設定に変更してください。SMARTACCESS による Windows ログオンを使用する設定にして修理したり、ハードウェアの設定を変更したりすると、Windows にログオンできなくなることがあります。

重要

- SMARTACCESSによるWindowsログオンの設定については、次のマニュアルを参照してください。
  - 「SMARTACCESS/Basic」をお使いの場合
    添付の「ドライバーズディスク」内にある「SMARTACCESS/Basic リファレンスマニュアル」
  - 「SMARTACCESS/Premium」をお使いの場合
    添付の「SMARTACCESS/Premium」CD-ROM 内にある「SMARTACCESS/Premium リファレンスマニュアル」

□ BIOS パスワードを解除する

「BIOS の設定を変更する」(→ P.12)で設定したパスワードを解除してください。

■修理後に必要な作業

□ リストアする

「リストアについて」(→ P.18)の処理に従って、鍵を復元してください。

□ BIOS パスワードを設定する

「BIOS の設定を変更する」(→ P.12)の手順 1 〜 6 に従って、パスワードを設定してください。

□ SMARTACCESS による Windows ログオンを使用する設定に変更する

SMARTACCESS による Windows ログオンを使用していた場合は、「SMARTACCESS/Basic リファレンスマニュアル」、または「SMARTACCESS/Premium リファレンスマニュアル」に従って、SMARTACCESS による Windows ログオンを使用する設定に変更してください。
なお、SMARTACCESS による Windows ログオンの設定を変更する前に、「現在の機器構成情報の登録」を行う必要があります。

パソコンの廃却について

パソコンを廃却する前に安全のため、次の手順に従ってセキュリティチップの鍵や、鍵に関連するファイルを削除してください。

重要

- セキュリティチップの鍵や、鍵に関連するファイルを削除すると、セキュリティチップにより保護されていた暗号化ファイルや証明書は利用できなくなります。
- セキュリティチップの鍵を削除すると、セキュリティチップで暗号化したファイルや証明書が利用できなくなります。
  削除する前に、必要に応じて暗号化ファイルを解除してください。

1. **「セキュリティチップの鍵を消去するには」（→ P.24）の手順に従って、セキュリティチップの鍵を消去します。**
2. **パソコン本体の『FMV マニュアル』の「セキュリティ」－「パソコン本体廃棄時のセキュリティ」をご覧になり、ハードディスク内のデータを削除します。**

6 こんなときには

重要

- セキュリティチップの設定の変更方法については、次のマニュアルをよくお読みになり、手順に従って設定してください。
  - 「SMARTACCESS/Basic」をお使いの場合
    添付の「ドライバーズディスク」内にある「SMARTACCESS/Basic リファレンスマニュアル」
  - 「SMARTACCESS/Premium」をお使いの場合
    添付の「SMARTACCESS/Premium」CD-ROM 内にある「SMARTACCESS/Premium リファレンスマニュアル」

パスワードを変更するには

セキュリティチップに設定した、所有者パスワードおよびユーザーキーパスワードは変更することが出来ます。また、ユーザーキーパスワードは各ユーザで定期的に変更することをお勧めします。
所有者パスワードの変更については、「SMARTACCESS/Basic リファレンスマニュアル」、または「SMARTACCESS/Premium リファレンスマニュアル」の「管理者ツール」の項目をご覧ください。
ユーザーキーパスワードの変更については、「SMARTACCESS/Basic リファレンスマニュアル」、または「SMARTACCESS/Premium リファレンスマニュアル」の「利用者ツール」の項目をご覧ください。

パスワードを忘れた場合には

ユーザーキーパスワードを忘れた場合は、再設定することができます。
ユーザーキーパスワードを再設定する場合には、所有者が再設定を行う承認処理を行った後、各ユーザで新しいパスワードを設定し直します。
パスワードをリセットする場合は、「SMARTACCESS/Basic リファレンスマニュアル」、または「SMARTACCESS/Premium リファレンスマニュアル」の「管理者ツール」の項目を参照してください。

セキュリティチップの鍵を消去するには

パソコンを廃却する場合には、パソコンに残ったデータを復元できないようにすることが重要です。セキュリティチップにより保護されたデータは、セキュリティチップ内のデータを破棄し、復元用ファイルを破棄することで再び復元することができなくなります。
セキュリティチップ内のデータを消去するには、次の手順で行います。

・「W5210 の場合」(→ P.24)
・「E5210、D5310、D5210、D5110、B5210、K5210、N5210FA の場合」(→ P.25)
・「FMV-LIFEBOOK、FMV-STYLISTIC の場合」(→ P.25)

重要

- この操作ではセキュリティチップのデータを破棄するだけで、ハードディスクのデータは破棄されません。
- セキュリティチップのデータを破棄したことで、ハードディスク内のセキュリティチップで保護されたデータは見ることができなくなりますが、実際の廃却時にはハードディスクのデータをクリアしてください。
- BIOS セットアップで、セキュリティチップ関連の設定を行うには、管理者用パスワードを設定する必要があります（W5210 以外の場合）。
- BIOS セットアップについて詳しくは、パソコン本体の『FMV マニュアル』の「BIOS」を参照してください。

■ W5210 の場合

1. **パソコン本体の電源を入れ、BIOS セットアップを起動します。**
   BIOS セットアップ画面が表示されます。
2. **Security メニューで、【Alt】＋【S】キーを押します。**
   「Clear Security Chip」の項目が設定可能になります。
3. **【↑】キーまたは【↓】キーを押して「Clear Security Chip」を選択し、【Enter】キーを押します。**
   設定変更画面が表示されます。
4. **【↑】キーまたは【↓】キーを押して「Enabled」に設定します。**
5. **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**
6. **【↑】キーまたは【↓】キーを押して「Save Changes & Exit」を選択し、【Enter】キーを押します。**
   「Save Configuration Changes and exit now?」が表示されます。
7. **【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。**
   BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- セキュリティチップの設定を有効にするには、BIOSセットアップ終了後にパソコン本体の再起動が必要です。

■ E5210、D5310、D5210、D5110、B5210、K5210、N5210FA の場合

1 **「BIOS の設定を変更する」－「E5210、D5310、D5210、D5110、B5210、K5210、N5210FA の場合」（→ P.13）の手順 1 ～ 6 を行います。**

2 **【↑】キーまたは【↓】キーを押して、「Clear Security Chip」を選択し、【Enter】キーを押します。**
クリアを続行してよいかを確認するウィンドウが表示されます。

3 **「Yes」を選択し、【Enter】キーを押します。**

4 **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**

5 **【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。**
「Save Configuration Changes and exit now?」が表示されます。

6 **【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。**
BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- 「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「Exit Saving Changes」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

■ FMV-LIFEBOOK、FMV-STYLISTIC の場合

1 **「BIOS の設定を変更する」－「FMV-LIFEBOOK、FMV-STYLISTIC の場合」（→ P.14）の手順 1 ～ 6 を行います。**

2 **【↑】キーまたは【↓】キーを押して、「セキュリティチップのクリア」を選択し、【Enter】キーを押します。**
クリアを続行してよいかを確認するウィンドウが表示されます。

3 **「はい」を選択し、【Enter】キーを押します。**

4 **【↑】キーまたは【↓】キーを押して、「セキュリティチップ」を選択します。**

5 **【Space】キーまたは【－】キーを押して、「使用しない」を選択します。**

6 終了メニューが表示されるまで、何度か【Esc】キーを押します。

7 【↑】キーまたは【↓】キーを押して「変更を保存して終了する」を選択し、【Enter】キーを押します。

「セットアップ確認」が表示されます。

8 【←】キーまたは【→】キーを押して「はい」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- 「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「変更を保存する」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

離席時にパソコンをロックするには

パソコンから離れる場合は、他人にパソコンを操作されないよう注意が必要です。
次の設定を行うことで、離席時でもパソコンはセキュリティチップにより安全に保護されます。

POINT

- 各設定方法については、Windows のマニュアルを参照してください。

■スクリーンセーバーのパスワード

スクリーンセーバーを設定する場合、「パスワードによる保護」を行うと、パスワードはセキュリティチップにより安全に保護されます。

■コンピュータのロック

「コンピュータのロック」を行うと、復帰時のパスワードはセキュリティチップにより安全に保護されます。

■スタンバイや休止状態から回復するときのパスワード

スタンバイや休止状態の設定をしている場合、「スタンバイから回復するときにパスワードの入力を求める」を設定しておくと、パスワードはセキュリティチップにより安全に保護されます。

新しいユーザを登録するには

Windows に新規ユーザを追加する場合、そのユーザがセキュリティチップを利用するためには、セキュリティチップに新規ユーザの情報を登録する必要があります。SMARTACCESS では Windows へ新規ユーザを追加し、セキュリティチップの登録を行うことが出来ます。

7 トラブルシューティング

□ BIOS でセキュリティチップの設定を変更できない（W5210 以外の場合）

BIOS で、セキュリティチップの使用や、セキュリティチップのデータをクリアする設定を行うためには、管理者用パスワードの設定が必要です。管理者用パスワードが設定されているか確認してください。

□ ソフトウェアがインストールできない

ソフトウェアをインストールするには、BIOS でセキュリティチップを使用する設定になっている必要があります。BIOS の設定を確認してください。

□ SMARTACCESS が起動できない

SMARTACCESS を起動するには、ソフトウェアが正常にインストールされ、設定が正常に終了している必要があります。

□ Windows ログオン時に機器が変更された旨のエラーメッセージが表示される

前回の起動からハードウェアの構成や設定が変更された可能性があります。ハードウェア構成や BIOS 設定など変更されていないか確認してください。変更があった場合は、機器を登録したときの状態に戻してください。
なお、変更の内容によっては、機器を登録したときの状態に戻しても、エラーメッセージが解除されない場合があります。詳細は「機器監査について」（→ P.19）を参照してください。

□ Windows ログオン時にユーザーキーパスワードエラーになる

SMARTACCESS による Windows ログオンを有効にしている場合には、Windows のパスワードではなくセキュリティチップのユーザーキーパスワードを入力してください。

□ EFS が利用できない

EFS を利用するにはハードディスクが NTFS でフォーマットされていることが必要です。FAT32 のドライブでは EFS を利用することはできません。なお、Windows XP Home Edition では、EFS は利用できません。

□ セキュリティチップを「Disabled」（FMV-ESPRIMO、FMV FA パソコンの場合）または「使用しない」（FMV-LIFEBOOK、FMV-STYLISTIC の場合）に設定すると、Windows にログオンできなくなった

SMARTACCESS による Windows ログオンを設定した状態で、セキュリティチップを「Disabled」（FMV-ESPRIMO、FMV FA パソコンの場合）または「使用しない」（FMV-LIFEBOOK、FMV-STYLISTIC の場合）に設定すると、セキュリティチップに保存していた Windows パスワードが利用できず、Windows にログオンできなくなる場合があります。
その場合はセキュリティチップを「Enabled」（FMV-ESPRIMO、FMV FA パソコンの場合）または「使用する」（FMV-LIFEBOOK、FMV-STYLISTIC の場合）に設定し直すか、「回避パスワード」でログオンする必要があります。なお、「回避パスワード」でログオンしても、セキュリティチップで保護された環境は安全に管理されています。

□ ハードウェア構成を変更したために Windows にログオンできなくなった

ハードウェアの構成を変更すると、SMARTACCESS の機器監査機能により Windows にログオンできなくなります。その場合はハードウェア構成を登録したときの設定に戻すか、機器構成を登録しなおす必要があります。設定方法については、「SMARTACCESS/Basic」をお使いの場合は添付の「ドライバーズディスク」内にある「SMARTACCESS/Basic リファレンスマニュアル」を、「SMARTACCESS/Premium」をお使いの場合は添付の「SMARTACCESS/Premium」CD-ROM 内にある「SMARTACCESS/Premium リファレンスマニュアル」をご覧ください。

□ SMARTACCESS による Windows ログオンでパスワードの入力画面が 2 度表示される

「ユーザーキーパスワード」と「一時中止パスワード」を同じにしている可能性があります。管理者にご相談ください。

□「リストアについて」を行うとユーザーキーパスワードが変わることがある

「リストアについて」(→ P.18)の処理を行った場合、ユーザーキーパスワードには、バックアップを行った時点でのパスワードが設定されます。
そのため、バックアップ後にユーザーキーパスワードを変更しても、復元すると、バックアップを行った時点でのパスワードに戻ります。

□ ソフトウェアのインストール時に「アプリケーションエラー」が表示されることがある

「SMARTACCESS/Basic」または「SMARTACCESS/Premium」のマニュアルの手順に従ってソフトウェアをインストールしない場合、「アプリケーションエラー」が表示されることがあります。
もし表示された場合、ソフトウェアのインストールを引き続き行い、インストール終了後は表示画面に従って Windows を再起動してください。再起動後は正常に動作します。

□ SMARTACCESS でユーザ初期化を行うと、失敗することがある

SMARTACCESS をインストール時に、セキュリティチップがクリアされていない状態で行うと、ユーザ初期化に失敗することがあります。インストール時にはセキュリティチップがクリアされていたかどうか確認してください。クリアされていなかった場合には SMARTACCESS をアンインストールし、BIOS でセキュリティチップをクリアした後、再度 SMARTACCESS をインストールしてください。

FMV シリーズ
セキュリティチップ
取扱説明書

B6FH-7991-04 Z2-00

発 行 日　2006 年 1 月
発行責任　富士通株式会社